IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Massimiliano Antonio Poletto et al.	Art Unit	: 2134
Serial No.	: 10/066,252	Examiner	: Nalven Andrew, I
Filed	: January 31, 2002	Conf. No.	: 2792
Title	: ARCHITECTURE TO THWART DENIAL OF SERVICE ATTACKS		

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF ON BEHALF OF MASSIMILIANO ANTONIO POLETTO ET AL.

The Appeal Brief fee has previously been paid. If any additional charges or credits are due, please to Deposit Account No. 06-1050.

CERTIFICATE OF MAILING BY EFS-WEB FILING

I hereby certify that this paper was filed with the Patent and Trademark Office using the EFS-WEB system on this date: September 25, 2007

(i.) Real Party In Interest

The real party in interest in the above application is Mazu Networks, Inc.

(ii.) Related Appeals and Interferences

The appellant is not aware of any appeals or interferences related to the above-identified patent application.

(iii.) Status of Claims

This is an appeal from the decision of the Primary Examiner in an Office Action dated June 8, 2007, rejecting claims 1-17, 24, 25 and 27-34. The examiner also indicated that claims 18-23 were objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. There was not a claim 26 originally filed.

Accordingly, claims 1-17, 24, 25 and 27-34 are the subject of this appeal.

(iv.) Status of Amendments

Appellant filed a Reply to the Office Action dated May 12, 2006 to change the status of claim 20 to "original." Appellant also amended claims 1 and 11 to correct informalities pointed out by the examiner and corrected minor informalities in claim 3. Appellant also attempted to renumbered claims 27-34, as claims 26-33.

In an advisory action dated September 6, 2006, the examiner did not enter the attempted re-numbering of claims 27-34 electing instead to defer re-numbering by examiner's amendment upon allowance. Otherwise, the examiner indicated entry of the amendment. Accordingly, all substantive amendments have been entered. Appellant filed a Notice of Appeal on August 14, 2006, which was received by the Office on August 17, 2006.

In response to the Notice of Appeal Appellant filed two Appeal Brief, an original Appeal Brief and a corrected Appeal Brief. In response to the corrected Appeal Brief, the examiner issued the office action of June 6, 2007, from which Appellant again appeals.

Appellant has filed a new Notice of Appeal herewith.

In addition, Appellant has filed a Reply to the Office Action of June 6, 2007. This Reply clarifies the language of claims 1 and 16. This Reply awaits entry. However, this Appeal Brief reflects entry of these amendments since entry of the Amendment to the Office Action of June 6, 2007 is a matter of right, because the action of June 6, 2007 was a non-final action.

(v.) Summary of Claimed Subject Matter

Claim 1

One aspect of Appellant's invention is set out in claim 1 as a monitoring device disposed for thwarting denial of service attacks on a data center. ***"Referring to FIG. 1, an arrangement 10 to thwart denial of service attacks (DoS attacks) is shown."***[1] ***"Some or all of the deployed monitor devices in the arrangement are provisioned monitors."***[2]

Inventive features of claim 1 include a device, coupled to physical links between the data center and a network, with the device disposed to examine traffic entering or leaving that data center on the coupled physical links ***"Referring now to FIG. 2, the data center 20 has a plurality of links 21a-21n with the Internet 14. Each customer Ci (0 <= i < N, for N customers) of the data center is associated with a set of addresses Ai. The provisioned monitor has a notion of inbound and outbound packets, obtained directly from the physical link's transmit and receive ports."***[3] and collect statistical information on packets that are sent between the network and the data center over the coupled physical links for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from the coupled links that the provisioned monitor is coupled to. ***"Probes 26a-26n perform several functions such as sampling of packets and collect information pertaining to statistical properties of the packets."***[4] Additional support is given by: ***"A service provider that provides a provisioned monitor 26 could perform ingress filtering on traffic entering its network from customers downstream of the provisioned monitor. In this way, any outbound packets with unknown***

[1] Appellant's specification Page 4, lines 22-23.
[2] Id. Page 5, lines 29-30.
[3] Id. Page 7, lines 6-11.
[4] Id. Page 8, lines 10-13.

source addresses (not in any address of address space Ai) are considered to be originating from unprovisioned customers rather than being part of a spoofed DoS attack."[5]

Claim 7

Claim 7 claims another aspect of the invention. Claim 7 is directed to a method of thwarting denial of service attacks on a victim data center coupled to a network. **This feature is supported by the analogous feature of claim 1 and FIG. 7B.**

Inventive features of claim 7 include collecting, using a provisioned monitor statistical information on packets that are sent between a network and a plurality of customers of the data center by examining traffic on selected links in the data center as if the collecting were being performed on links that are downstream from the selected links that the provisioned monitor is disposed on. **This feature is supported as the analogous feature of claim 1.**

Inventive features of claim 7 also include communicating data, over a dedicated network, to a control center. This feature is supported as the analogous feature of claim 1 and ***"In some embodiments, the control center 24 is coupled to the gateways 26 and data collectors 28 by a hardened, redundant network 30. In preferred embodiments, the network is inaccessible to the attacker."***[6]

Claim 11

Another aspect of the invention is covered by claim 11. Claim 11 is directed to an arrangement to monitor a link between a data center and a network for thwarting denial of service attacks on the data center. **This feature is supported by the analogous feature of claim 1.**

Inventive features of claim 11 include, a provisioned monitor, placed on selected links in the data center so that the provisioned monitor examines traffic entering or leaving that data center on the selected links and collects statistical information for a plurality of provisioned customers, which are on links that are downstream from the selected links that the provisioned monitor is disposed on, This feature is supported by the analogous feature of claim 1. The provisioned monitor maintaining separate counter logs for each provisioned customer. ***"Each***

[5] Id. Page 7, lines 22-28.
[6] Appellant's specification Page 5, lines 16-20.

provisioned monitor keeps separate counter logs 52a-52d for each provisioned customer (virtual monitor)."[7]

Inventive features of claim 11 also include a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to. ***"... as well as a global counter log 52 that accounts for all traffic seen on the link."*** [8]

Claim 24

Claim 24 is directed a method of thwarting attacks on a victim data center coupled to a network. **This feature is supported by the analogous feature of claim 1 and FIG. 7B.**

Inventive features of claim 24 include collecting statistical information for a plurality of provisioned customers on links that are downstream from links on which collecting occurs. ***"Referring now to FIG. 2, the data center 20 has a plurality of links 21a-21n with the Internet 14. Each customer Ci (0 <= i < N, for N customers) of the data center is associated with a set of addresses Ai. The provisioned monitor has a notion of inbound and outbound packets, obtained directly from the physical link's transmit and receive ports."***[9]

Inventive features of claim 24 include maintaining separate counter logs for each provisioned customer ***"Each provisioned monitor keeps separate counter logs 52a-52d for each provisioned customer (virtual monitor)."***[10] **and a global counter log that accounts for all traffic seen on the links on which collecting occurs.** ***"...Another embodiment (not shown) maintains duplicate packets, keeping both a global packet log and one log for each virtual monitor,."***[11]

Claim 29

Claim 29 is directed to a method of thwarting attacks on a victim data center coupled to a network. **This feature is supported as the analogous feature of claim 1.**

---

[7] Id. Page 11, lines 29-31.
[8] Id. Page 11, lines 31-32.
[9] Appellant's specification Page 7, lines 6-11.
[10] Id. Page 11, lines 29-31.
[11] Id. Page 12, lines 5-7.

Inventive features of claim 29 include collecting statistical information for a plurality of links that are downstream from links on which collecting occurs. **This feature is supported as the analogous feature of claim 1.**

Inventive features of claim 29 include performing traffic analysis on the collected statistical information on a per downstream link basis to identify malicious traffic. ***"Packet analysis for a particular virtual monitor happens by classifying packets based on addresses at the time of the analysis."***[12]

Inventive features of claim 29 also include communicating alerts that arise from the traffic analysis. ***"The method also includes communicating alerts that arise from the traffic analysis."***[13]

(vi.) Grounds of Rejection to be Reviewed on Appeal

1. Claim 1 stands rejected under 35 U.S.C. 112, second paragraph as being indefinite.

2. Claims 1, 5, 11, 24, 27 stand rejected under 35 U.S.C. 102(a) as being anticipated by Mansfield "Towards trapping wily intruders in the large."

3. Claims 2-3, 7, 9-10, and 33 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield "Towards trapping wily intruders in the large" in view of Crosbie et al US Pub 2002/0083343.

4. Claims 4, 6, 12-15, 25, 28-32, and 34 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield "Towards trapping wily intruders in the large" in view of Kim US Pub 2002/0069356.

5. Claim 8 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield "Towards trapping wily intruders in the large" and Crosbie et al US Pub 2002/0083343, as applied to claim 7 above, and in further view of Kim US Pub 2002/0069356.

---

[12] Id. Page 12, lines 3-5.
[13] Appellant's specification Page 2, line 31 to page 3, line 2.

6. Claim 16 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield "Towards trapping wily intruders in the large" and Kim US Pub 2002/0069356, as applied to claim 13 above, and in further view of Gales US Pub 2003/0084323.

7. Claim 17 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Mansfield "Towards trapping wily intruders in the large" and Kim US Pub 2002/0069356, as applied to claim 13 above, and in further view of Syvanne et al US Patent No. 7,162,737 and Gales US Pub 2003/0084323.

(vii.) Argument

Anticipation

"It is well settled that anticipation under 35 U.S.C. §102 requires the presence in a single reference of all of the elements of a claimed invention." *Ex parte Chopra*, 229 U.S.P.Q. 230, 231 (BPA&I 1985) and cases cited.

"Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim." *Connell v. Sears, Roebuck & Co.*, 220 U.S.P.Q. 193, 198 (Fed. Cir. 1983).

"This court has repeatedly stated that the defense of lack of novelty (i.e., 'anticipation') can only be established by a single prior art reference which discloses each and every element of the claimed invention." *Structural Rubber Prod. Co. v. Park Rubber Co.*, 223 U.S.P.Q. 1264, 1270 (Fed. Cir. 1984), citing five prior Federal Circuit decisions since 1983 including *Connell.*

In a later analogous case the Court of Appeals for the Federal Circuit again applied this rule in reversing a denial of a motion for judgment n.o.v. after a jury finding that claims were anticipated. *Jamesbury Corp. v. Litton Industrial Prod., Inc.*, 225 U.S.P.Q. 253 (Fed. Cir. 1985).

After quoting from *Connell*, "Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim," 225 U.S.P.Q. at 256, the court observed that the patentee accomplished a constant tight contact in a ball valve by a lip on the seal or ring which interferes with the placement of the ball. The lip protruded into the area where the ball will be placed and was thus deflected after the ball was assembled into the valve. Because of this constant pressure, the patented valve was described as providing a

particularly good seal when regulating a low pressure stream. The court quoted with approval from a 1967 Court of Claims decision adopting the opinion of then Commissioner and later Judge Donald E. Lane:

> [T]he term "engaging the ball" recited in claims 7 and 8 means that the lip contacts the ball with sufficient force to provide a fluid tight seal **** The Saunders flange or lip only sealingly engages the ball 1 on the upstream side when the fluid pressure forces the lip against the ball and never sealingly engages the ball on the downstream side because there is no fluid pressure there to force the lip against the ball. The Saunders sealing ring provides a compression type of seal which depends upon the ball pressing into the material of the ring. *** The seal of Saunders depends primarily on the contact between the ball and the body of the sealing ring, and the flange or lip sealingly contacts the ball on the upstream side when the fluid pressure increases. 225 U.S.P.Q. at 258.

Relying on *Jamesbury*, the ITC said, "Anticipation requires looking at a reference, and comparing the disclosure of the reference with the claims of the patent in suit. A claimed device is anticipated if a single prior art reference discloses all the elements of the claimed invention as arranged in the claim." *In re Certain Floppy Disk Drives and Components Thereof*, 227 U.S.P.Q. 982, 985 (U.S. ITC 1985).

Obviousness

"It is well established that the burden is on the PTO to establish a prima facie showing of obviousness, *In re Fritsch*, 972 F.2d. 1260, 23 U.S.P.Q.2d 1780 (C.C.P.A., 1972)."

In *KSR International Co. v. Teleflex Inc.*, __ U.S. __, 2007 WL 1237837 (Apr. 30, 2007), the Supreme Court reversed a decision by the Court of Appeal's for the Federal Circuit decision that reversed a summary judgment of obviousness on the ground that the district court had not adequately identified a motivation to combine two prior art references. The invention was a combination of a prior art repositionable gas pedal, with prior art electronic (rather than mechanical cable) gas pedal position sensing. The Court first rejected the "rigid" teaching suggestion motivation (TSM) requirement applied by the Federal Circuit, since the Court's

obviousness decisions had all advocated a "flexible" and "functional" approach that cautioned against "granting a patent based on the combination of elements found in the prior art."

With respect to the genesis of the TSM requirement, the Court noted that although "As is clear from cases such as Adams[14], a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. Although common sense directs one to look with care at a patent application that claims as innovation the combination of two known devices according to their established functions, it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does. This is so because inventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known."

In application of the TSM requirement, the Court cautioned that: "Helpful insights, however, need not become rigid and mandatory formulas; and when it is so applied, the TSM test is incompatible with our precedents."

The court also addressed the application of the TSM test: "In the years since the Court of Customs and Patent Appeals set forth the essence of the TSM test, the Court of Appeals no doubt has applied the test in accord with these principles in many cases. There is no necessary inconsistency between the idea underlying the TSM test and the Graham analysis. But when a court transforms the general principle into a rigid rule that limits the obviousness inquiry, as the Court of Appeals did here, it errs."

"The mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification." *In re Gordon*, 221 U.S.P.Q. 1125, 1127 (Fed. Cir. 1984).

> Although the Commissioner suggests that [the structure in the primary prior art reference] could readily be modified to form the [claimed] structure, "[t]he mere fact that the prior art could be so modified would not have made the modification obvious unless the

[14] United States v. Adams, 383 U. S. 39, 40 (1966)

> prior art suggested the desirability of the modification." *In re Laskowski*, 10 U.S.P.Q. 2d 1397, 1398 (Fed. Cir. 1989).

"The claimed invention must be considered as a whole, and the question is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination." *Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick*, 221 U.S.P.Q. 481, 488 (Fed. Cir. 1984).

> Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination. Under Section 103, teachings of references can be combined only if there is some suggestion or incentive to do so. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984) (emphasis in original, footnotes omitted).

"The critical inquiry is whether 'there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination.'" *Fromson v. Advance Offset Plate, Inc.*, 225 U.S.P.Q. 26, 31 (Fed. Cir. 1985).

1. Claim 1 is proper under 35 U.S.C. 112, second paragraph.

Appellant has enclosed an amendment that addresses this rejection and clarifies language in the claims.

2. Claims 1, 5, 11, 24, 27 are not anticipated by Mansfield "Towards Trapping Wily Intruders in the Large."

Claims 1 and 5

For the purposes of this appeal only, claims 1 and 5 stand or fall together. Claim 1 is representative of this group of claims.

Claim 1 is directed to a monitoring device disposed for thwarting denial of service attacks on a data center. Claim 1 includes the feature of a device, coupled to physical links between the

data center and a network, with the device disposed to examine traffic entering or leaving that data center on the coupled physical links and collect statistical information on packets that are sent between the network and the data center over the coupled physical links for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from the coupled links that the provisioned monitor is coupled to.

The examiner contends that:

> **With regards to claim 1, Mansfield teaches a device, coupled to physical links between the data center and a network, with the device disposed to examine traffic entering or leaving that data center on the coupled physical links (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link) and collect statistical information on packets that are sent between a network and the data center for a plurality of customers (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites. Figure 4, sites 1,2,3, and 4) by examining traffic as if the device was disposed on links that are downstream from the links that the provisioned monitor is on (Mansfield, page 6 Section 3.1, traffic monitors traffic entering each site).**

Appellant disagrees. Mansfield fails to describe or suggest a device, coupled to physical links between the data center and a network ..., that ... collects statistical information on packets that are sent between the network and the data center ... for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from links that the provisioned monitor is coupled to. Rather, Mansfield discloses signature-based traffic tracing.[15]

Mansfield describes a system to collect relevant packet count information from each link, which connects to the sites.[16] However, nowhere does Mansfield disclose a device... disposed to examine traffic entering or leaving that data center on the coupled physical links. In particular, Mansfield does not disclose a device that collects statistical information on packets, for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from the links that the provisioned monitor is coupled to.

Appellant contends that the examiner has not fully considered all of the limitations of claim 1. Specifically, Appellant contends that the examiner does not consider the feature that the device is coupled to physical links between the data center and the network and that the device is

---

[15] Mansfield page 6.
[16] Id.

disposed to examine traffic entering or leaving that data center ... as if the device was disposed on links that are downstream from the coupled links that the provisioned monitor is coupled to.

The Examiner points to Mansfield's teachings at page 6 Section 3.1, for the feature of "a device, coupled to physical links between the data center and a network" and for the feature of "... examining traffic as if the device was disposed on links that are downstream from the links that the provisioned monitor is on." The excerpt from Mansfield is reproduced below:

3.1 Traffic-flow signatures

The basic concept of signature-based traffic tracing is shown in Fig.4. The traffic monitor collects the relevant packet count information from each link, which connects the sites. The NMS compares the monitored traffic pattern, and correlates them. The correlated chain of patterns indicates the path of (probably spoofed) traffic-flow. It should be noted that the information used is packet count only, neither packet capture nor analysis is needed.

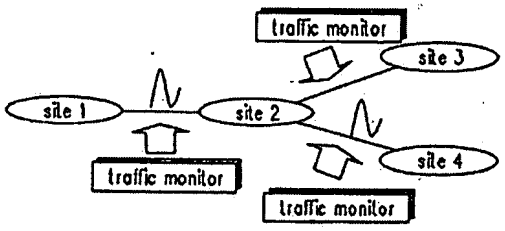

Fig. 4 Concept of pattern based traffic tracing

In this excerpt, Mansfield shows traffic monitors deployed at points in a network between sites 1-4.[17] Mansfield neither shows that the monitors are coupled to physical links between the network and the data center nor does Mansfield describe or suggest on page 6 or elsewhere this feature. Mansfield only shows traffic monitors disposed in a network[18]. Mansfield also fails to show or describe that the device examines traffic entering or leaving that data center on the coupled physical links.

While Mansfield arguable shows that traffic monitors collect statistical information on packets (e.g., the number of packets), Mansfield does not specifically describe that the collected

[17] Appellant contends that Figure 4 more likely shows a model related to tracing, rather than an actual network implementation.

[18] See Mansfield Figure 6 for confirmation.

statistical information is collected according to packets that are sent between the network and the data center over the coupled physical links for a plurality of customers. In addition, Mansfield clearly does not show that collection occurs "by examining traffic as if the device was disposed on links that are downstream from the coupled links that the provisioned monitor is coupled to."

Accordingly, since Mansfield fails to describe all of the features of claim 1, arranged as in the claim, Mansfield cannot anticipate claim 1.

Claim 11

Claim 11 calls an arrangement disposed to monitor a link between a data center and a network for thwarting denial of service attacks on the data center. Claim 11 includes a provisioned monitor, placed on selected links in the data center ... that ... examines traffic entering or leaving that data center ... and collects statistical information for a plurality of provisioned customers ... the provisioned monitor maintaining separate counter logs for each provisioned customer and a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to.

Claim 11 includes the feature of a provisioned monitor that collects statistical information for a plurality of provisioned customers, which for reasons discussed above is neither described nor suggested by Mansfield. In addition, claim 11 includes the feature that the provisioned monitor maintains separate counter logs for each provisioned customer and a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to.

The examiner contends that:

> **With regards to claims 11, Mansfield teaches a provisioned monitor placed on selected links in the data center so that the provisioned monitor examines traffic entering or leaving the data center on the selected links (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link) and collect statistical information for a plurality of provisioned customers which are on links that are downstream from links that the provisioned monitor is on (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites. Figure 4, sites 1, 2, 3, and 4), the provisioned monitor maintaining separate counter logs for each provisioned customer (Mansfield, page 6, traffic monitor collects information from link) and a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8)**

In formulating reasons for rejection of claim 11, the examiner improperly reads into Mansfield features that are neither shown nor described by Mansfield. Claim 11 calls for the feature of: " a provisioned monitor, placed on selected links in the data center ..." The examiner argues that "**(Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link).**" Mansfield does not describe that the "links" disclosed by Mansfield are between the network and the data center. Rather, the "links" in Figure 4 are network paths between different sites that are coupled by the network. Concomitant therewith, Mansfield also does not describe that: "the provisioned monitor examines traffic entering or leaving that data center on the selected links." While Mansfield arguable describes statistical information, Mansfield does not describe collecting statistical information "for a plurality of provisioned customers."

Claim 11 also includes the features of: "maintaining separate counter logs for each provisioned customer; and a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to."

Mansfield clearly does not teach the feature of: "... the provisioned monitor maintaining separate counter logs for each provisioned customer." Mansfield does not specifically suggest, much less describe, separate counter logs for each provisioned customer. The examiner argues that Mansfield teaches the separate counter logs for each provisioned customer because **(Mansfield, page 6, traffic monitor collects information from link).**[19] However, this does not describe or suggest that the statistical information collected by Mansfield is maintained in separate counter logs on a provisioned customer basis.

Likewise, Mansfield does not describe a global counter log that accounts for all traffic seen on the link. The examiner argues that this feature is taught by **(Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8).** However, the claimed global counter log is provided to account for all traffic seen on a link that connects the data center to the network. Mansfield shows a graph (not a global counter) that combines traffic between two sites, not all traffic seen on the link.

Accordingly Mansfield cannot anticipate claim 11, Mansfield does not identically describe each element of claim 11 arranged as in the claim.

---

[19] Examiner's action page 4.

Claims 24 and 27

For the purposes of this appeal only, claims 24 and 27 stand or fall together. Claim 24 is representative of this group of claims.

Claim 24 distinguishes over Mansfield since the reference fails to describe "... collecting statistical information for a plurality of provisioned customers on links that are downstream from links on which collecting occurs and maintaining separate counter logs for each provisioned customer, and a global counter log that accounts for all traffic seen on the links on which collecting occurs."

According to the examiner:

> **With regards to claim 24, Mansfield teaches collecting statistical information for a plurality of provisioned customers on links that are downstream from links on which collecting occurs (Mansfield, page 6 Section 3.1, traffic monitors collect relevant packet count information from each link for multiple sites. Figure 4, sites 1,2,3, and 4) and maintaining separate counter logs for each provisioned customer (Mansfield, page 6, traffic monitor collects information from link) and a global counter log that accounts for all traffic seen on the links on which collecting occurs (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8).**

The examiner uses the same reasoning to reject claim 24, as was used to reject claim 11. The examiner contends with respect to these later features of the logs that Mansfield teaches:

"...maintaining separate counter logs for each provisioned customer (Mansfield, page 6, traffic monitor collects information from link) and a global counter log that accounts for all traffic seen on the links on which collecting occurs (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8)."

Mansfield does not specifically suggest, much less describe collecting statistical information for a plurality of provisioned customers on links that are downstream from links on which collecting occurs and maintaining separate counter logs for each provisioned customer, as was argued above for claim 11.

Moreover Mansfield does not suggest much less describe the featured global counter log that accounts for all traffic seen on the links on which collecting occurs.

As with claim 11 which recites "a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to" Mansfield, at page 6 (set for above in the

discussion of claim 11) and page 9, neither describes nor suggests "a global counter log that accounts for all traffic seen on the links on which collecting occurs, as called for by claim 24."[20]

Therefore, Mansfield also cannot anticipate claim 24.

3. Claims 2-3, 7, 9, 10, and 33 are allowable over Mansfield in view of Crosbie et al US Pub 2002/0083343.

Claims 2 and 3

For the purposes of this appeal only, claims 2 and 3 stand or fall together. Claim 2 is representative of this group of claims.

Claim 2 further limits claim 1, and recites that: "the monitoring device is coupled to a control center through a dedicated, private network.[21] The examiner argues that:

> **With regards to claim 2, Mansfield fails to teach the monitoring device being coupled to a control center through a dedicated private network. However, Crosbie teaches the monitoring device being coupled to a control center through a dedicated private network (Crosbie, paragraph 0116-0118, SSL connection between management station and agent systems). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Crosbie's method of securing communication because it offers the advantage of preventing unauthorized modification or deletion of data as it flows across the network and helps detect when an interloper sends messages which purport to be from another machine (Crosbie, paragraph 0117).**

This feature is neither described nor suggested by Mansfield, as the examiner acknowledges. Appellant contends however that this feature is also not disclosed by Crosbie or the combination of Crosbie with Mansfield. The examiner argues that: "**Crosbie teaches the monitoring device being coupled to a control center through a dedicated private network (Crosbie, paragraph 0116-0118, SSL connection between management station and agent systems).**"

---

[20] Appellant's specification pages 11 and 12 delineate different embodiments. See also notes 8 and 11, above.

[21] Appellant's specification page 16, lines 4-12:

> The gateway 26 uses a separate interface over a private, redundant network, such as a modem 39 over the telephone network or a leased line, a network adapter over a LAN, etc. to communicate with the control center 24. Other interface types are possible. In addition, the gateway 26 can include processes (not shown) to allow an administrator to insert filters to block, i.e., discard packets that the device deems to be part of an attack, as determined by heuristics described below.

The advantage of this arrangement is to make communications with the control center inaccessible to the attacker and to avoid the problem of network traffic during an attack obfuscating communications among the control center and the monitors.

Crosbie in [0116]-[0119] discloses secure messaging and protocols, e.g., the Secure Socket Layer (SSL) protocol. However, that is a protocol not a dedicated, private network. Accordingly, no combination of Mansfield with Crosbie suggests the feature of claim 2.

Claims 7, 9 and 10

For the purposes of this appeal only, claims 7, 9 and 10 stand or fall together. Claim 7 is representative of this group of claims.

Claim 7 is directed to a method of thwarting denial of service attacks on a victim data center. Claim 7 includes the features of collecting, using a provisioned monitor statistical information on packets that are sent between a network and a plurality of customers of the data center by examining traffic on selected links in the data center as if the collecting were being performed on links that are downstream from the selected links that the provisioned monitor is disposed on and communicating data, over a dedicated network, to a control center.

Features of claim 7 include that collecting statistical information is performed using a provisioned monitor, where collection is performed on a provisioned customer basis as if the collection was being perform on links that were downstream from the links that the provisioned monitor is disposed on.

Mansfield fails to suggest a provisioned monitor, e.g., collection on a customer basis, and in particular does not discuss any concept of provisioning a device for collection of statistical data on a customer basis as if the collecting was occurring on links downstream from the links that the monitor is disposed on. As discussed in claim 1, Mansfield does not collect statistical information on packets sent between a network and a plurality of customers.

The examiner again turns to Crosbie to teach the feature of the dedicated network. However, for reasons already discussed, Crosbie does not teach a dedicated network for the control center but merely discloses the SSL protocol.

Claim 33

Claim 33 depends from claim 29 and requires that communicating occurs on a downstream link basis over a dedicated, hardened network to a control center that determines a response to the attack. The combination of Mansfield and Crosbie do not suggest the feature of

the dedicated network. While arguable, teaching of SSL in Crosbie suggests the feature that the network is "hardened," it does not suggest that the network is "dedicated." Moreover, the purpose of a dedicated network[22], as set out in the claims, is not met by the motivation[23] offered by the examiner, thus showing a clear lack of suggestion to combine these references under *KSR*, since any proper exercise of common sense would tell the person of ordinary skill in this art that the secure socket layer protocol would still have packets that traverse portions of the network that is being monitored by the monitoring device thus potentially disrupting communications between the monitoring device and the control center.

4. Claims 4, 6, 12-15, 25, 28-32, and 34 are patentable over Mansfield in view of Kim US Pub 2002/0069356.

Claim 4

Claim 4, further limits claim 1, by requiring that the monitoring device is a gateway device and that it includes a process to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack. The examiner contends that:

> **With regards to claim 4, Mansfield teaches a process to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack (Mansfield, page 10, security manager uses network information to trap or track down intruder), but fails to teach the monitoring device is a gateway device. However, Kim teaches that the monitoring device is a gateway device (Kim, Abstract, integrated security gateway). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Kim's method of using a gateway because it offers the advantage of reducing costs by integrated security elements and increase security by reducing the amount of elements that may be attacked (Kim, paragraphs 0012-0013).**

The examiner clearly acknowledges that Mansfield does not teach that the device is a gateway. As the term "gateway" is used by Appellant and Kim, the gateway is disposed between a router and server systems (e.g., data center).

---

[22] See note 1 above.

[23] "...because it offers the advantage of preventing unauthorized modification or deletion of data as it flows across the network and helps detect when an interloper sends messages which purport to be from another machine (Crosbie, paragraph 0117)." (Examiner's Action page 7).

In essence, the examiner's reasoning is to simple re-name Mansfield's monitoring devices as gateways. However, Appellant contends that to re-name Mansfield's approach as a gateway device does not justify combining the references, since Mansfield is concerned with deployed monitors in a network and not with devices deployed to monitor links between a network and a data center. Thus, renaming Mansfield's arrangement as a gateway, still does not suggest this feature of claim 4.

Moreover, neither Mansfield nor Kim mention to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack. While Kim clearly discloses filtering, the filters are not for removing traffic that is deemed to be part of an attack. Rather the filtering disclosed by Kim is filtering based upon security associations attached to packets. Therefore, no combination of Mansfield with Kim describes or suggests "to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack."

Claim 6

Claim 6 further limits claim 4 to require that the gateway includes "a process to aggregate traffic from the various links and to produce logs and detection heuristics."

The examiner argues that: **"With regards to claim 6, Mansfield as modified teaches a process to aggregate traffic from the various links and to produce logs and detection heuristics (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8)."**

Appellant disagrees. At the outset, Appellant points out that Kim has been used in rejection of this particular feature of claim 6.

Mansfield, as argued above, does not appear to aggregate traffic from the claimed links to produce detection heuristics. While Mansfield shows counts from probe 1 and probe 2, there is no suggestion that this so called "aggregation" as the examiner characterizes it, is performed by a process that operates on the claimed gateway. Thus, claim 6 further distinguishes over Mansfield and Kim.

Claim 12

Claim 12 depends from claim 11, and calls for the provisioned monitor is a gateway that maintains separate packet logs for each monitor.

As argued above there is no suggestion to modify Mansfield to make the monitors of Mansfield gateways. Moreover, Mansfield does not describe the packet logs maintained for each monitor, and Kim does not cure that deficiency.

Claim 13

Claim 13 serves to further distinguish the arrangement of claim 12 by requiring that the gateway maintains a global packet log for all traffic. No combination of Mansfield with Kim either describes or suggests the global packet log for analogous reasons discussed above. Mansfield does not disclose a global packet log and Kim does not cure the deficiencies in Mansfield.

Claims 14 and 15

For the purposes of this appeal only, claims 14 and 15 stand or fall together. Claim 14 is representative of this group of claims.

Claim 14 limits claim 13 to require that the global packet log include a sample of all traffic seen on the link to which the gateway is connected. Mansfield does not describe the global packet log and does not describe any feature associated with the Figure 8 that depicts "**combines counts from probe 1 and probe 2**"[24] as logs resulting from a sample of all traffic seen on a link that is monitored. Claim 14 therefore is not suggested by any purported combination of Mansfield with Kim.

Claim 25

Claim 25 distinguishes since the combination of references neither describes nor suggests that collecting occurs on a gateway that passes network packets, the gateway being disposed at an edge of the network.

---

[24] Mansfield Fig. 8.

Again, while Kim teaches a gateway, the examiner's motivation is merely to rename features of Mansfield as a gateway.

Claim 29

Claim 29 is directed to a method of thwarting attacks on a victim data center ... and includes collecting statistical information for a plurality of links that are downstream from links on which collecting occurs, performing traffic analysis on the collected statistical information on a per downstream link basis to identify malicious traffic and communicating alerts that arise from the traffic analysis.

Claim 29 distinguishes over any purported combination of Mansfield with Kim since the combination of references neither describes nor suggests the feature of "collecting" as discussed in claim 24, and in addition, the combination neither describes nor suggests "performing traffic analysis on the collected statistical information on a per downstream link basis to identify malicious traffic." Mansfield does not process statistical information on a per downstream link basis and Kim does not cure that deficiency.

Claims 30, 31, 32 and 34

Each of claims 30, 31, 32 and 34 add distinct features to distinguish claim 29 over Mansfield and Kim

For example, the combination of Mansfield and Kim neither describes nor suggests that performing analysis occurs on statistical information collected for an individual one of the downstream links to identify malicious traffic intended for the individual one of the downstream links, as in claim 30. The combination of Mansfield and Kim neither describes nor suggests that analysis is performed on traffic intended for an individual one of downstream links, e.g., to maintain provisioned DOS monitoring on a per customer basis.

Claim 31, requires that communicating to a control center occurs on a downstream link basis, which is neither described nor suggested by the combination of Mansfield and Kim. Figure 8 in Mansfield does not suggest any communication on a downstream link basis.

Claim 32, which requires that communicating occurs on a downstream link basis to a control center that determines a response to the attack, is not suggest by the combination of references.

Claim 34 is directed to filtering the identified malicious traffic and to eliminate the malicious traffic from reaching the one of the downstream links. Claim 34 is neither described nor suggested by any combination of Mansfield and Kim, for analogous reasons generally discussed in claim 4. Clearly, Mansfield does not teach any filtering at all, and although Kim mentions filtering based upon security associations attached to packets, does not suggest filtering of malicious traffic, as called for in claim 34.

5. Claim 8 is patentable over Mansfield, Crosbie and Kim.

Claim 8

Claim 8, which recites that the device is a gateway device and further includes installing filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack, is allowable for analogous reasons to those given in claim 4, since no combination of Mansfield and Kim suggest these features.

In addition, while Crosbie mentions filtering, the filtering taught by Crosbie is not packet based (removing network-traffic deemed part of an attack), but instead is directed to filtering of events,[25] filtering of data to reduce data processed by an IDS[26] or to reduce the number of alerts.[27] The filtering taught in Crosbie can be configured on a file basis.[28]

Accordingly no combination of Mansfield, Crosbie or Kim suggest claim 8.

---

[25] Crosbie, [0185] and [0195]
[26] Id. [0193]
[27] Id. [0204]
[28] Id. [0229] - [0233]

6. Claim 16 is patentable over Mansfield, Kim and Gales US Pub 2003/0084323.

Claim 16

Claim 16, limits the arrangement of claim 13, requiring that "...the gateway maintains duplicate packets, keeping both a global packet log and a packet log for each monitor."

According to the examiner:

> **With regards to claim 16, Mansfield as modified fails to teach the gateway maintaining duplicate packets keeping both a global packet log and a packet log for each virtual monitor. However, Gales teaches the gateway maintaining duplicate packets keeping both a global packet log and a packet log for each virtual monitor (Gales, paragraph 0016, network activity log for information about global network usage, paragraph 0018, activity profile data has information for each of the nodes including inbound and outbound communication data). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Gales' method of keeping duplicate logs because it offers the advantage of allowing determination of security events on both a network and particular node level (Gales, paragraphs 0021-0022).**

Mansfield combined with Kim fails to suggest the features of base claim 13, as argued above. Gales does not cure this deficiency in the purported combination. In addition, Gales does not disclose the claimed global packet log and packet log for each monitor. Rather, Gales discloses logs that are directed to tracking activity of nodes not packets traffic, as claimed in claim 16.

7. Claim 17 is patentable over Mansfield, Kim Syvanne et al and Gales.

Claim 17

Claim 17 further limits claim 12, and requires that the gateway is a clustered gateway and includes a plurality of probes and a cluster head, with the cluster head having a process to aggregate traffic from the probes and to produce separate counter logs for each provisioned customer; and a global counter log, and produce detection heuristics.

The examiner contends that:

> **With regards to claim 17, Mansfield as modified teaches a process to aggregate traffic from probes (Mansfield, page 9, combines counts from probe 1 and probe 2**

in Figure 8) and to produce a global counter log and produce detection heuristics (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8, page 8, looks for reply messages, page 9, looks for request messages. Figure 8, incoming and outgoing) and a node head (Mansfield, page 9, combines counts from probe 1 and probe 2 in Figure 8). Mansfield as modified fails to teach producing a separate counter log for each provisioned customer or the gateway being a clustered gateway with a plurality of probes. However, Gales teaches the gateway maintaining packet log for each virtual monitor (Gales, paragraph 0016, network activity log for information about global network usage, paragraph 0018, activity profile data has information for each of the nodes including inbound and outbound communication data).

Syvanne teaches the gateway being a clustered gateway with a plurality of probes (Syvanne, column 5 line 60 - column 6 line 10, clustered gateway). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Syvanne's cluster methodology and Gale's logging method because it offers the advantage of allowing determination of security events on both a network and particular node level (Gales, paragraphs 0021-0022) and allows the flexible and reliable synchronization of state information between nodes in a gateway cluster (Syvanne, column 4 lines 50-60).

No combination of Mansfield and Kim suggest the features of base claim 12. The examiner uses Gales to teaches the feature of packet log for each virtual[29] monitor. Gales does not teach the packet logs for reasons given above.

The examiner uses Syvanne to teach features of the clustered gateway **(Syvanne, column 5 line 60 - column 6 line 10, clustered gateway).** Appellant contends that Syvanne possess no teachings that would suggest much less describe a clustered gateway, a plurality of probes and a cluster head … , as claimed. Syvanne's security gateway cluster does not suggest the features of the claimed cluster, namely, "a plurality of probes and a cluster head, with the cluster head having a process to aggregate traffic from the probes."

[29] Virtual monitor is not recited in claim 17.

Conclusion

Appellant submits, therefore, that Claims 1-25 and 27-34 are allowable over the cited art. Therefore, the Examiner erred in rejecting Appellant's claims and should be reversed.

Respectfully submitted,

Date: 9/25/07

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21719385.doc

Appendix of Claims

1. A monitoring device disposed for thwarting denial of service attacks on a data center, the monitoring device comprising:

a device, coupled to physical links between the data center and a network, with the device disposed to examine traffic entering or leaving that data center on the coupled physical links and collect statistical information on packets that are sent between the network and the data center over the coupled physical links for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from the coupled links that the provisioned monitor is coupled to.

2. The monitoring device of claim 1 wherein the monitoring device is coupled to a control center through a dedicated, private network.

3. The monitoring device of claim 2 wherein the device further comprises:

a communication process that communicates the statistical information on packets with the control center, and which receives queries or instructions from the control center.

4. The monitoring device of claim 1 wherein the monitoring device is a gateway device and further comprises:

a process to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack.

5. The monitoring device of claim 1 wherein the monitoring device is a data collector device.

6. The monitoring device of claim 4 wherein the gateway comprises:

a process to aggregate traffic from the various links and to produce logs and detection heuristics.

7. A method of thwarting denial of service attacks on a victim data center coupled to a network comprises:

collecting, using a provisioned monitor statistical information on packets that are sent between a network and a plurality of customers of the data center by examining traffic on selected links in the data center as if the collecting were being performed on links that are downstream from the selected links that the provisioned monitor is disposed on; and

communicating data, over a dedicated network, to a control center.

8. The monitoring device of claim 7 wherein the device is a gateway device, which further comprises:

installing filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack.

9. The monitoring device of claim 7 wherein the monitoring device is a data collector device.

10. The monitoring device of claim 7 wherein collecting occurs for inbound and/or outbound traffic.

11. An arrangement disposed to monitor a link between a data center and a network for thwarting denial of service attacks on the data center, the arrangement comprising:

a provisioned monitor, placed on selected links in the data center so that the provisioned monitor examines traffic entering or leaving that data center on the selected links and collects statistical information for a plurality of provisioned customers, which are on links that are downstream from the selected links that the provisioned monitor is disposed on, the provisioned monitor maintaining separate counter logs for each provisioned customer; and

a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to.

12. The arrangement of claim 11 wherein the provisioned monitor is a gateway that maintains separate packet logs for each monitor.

13. The arrangement of claim 12 wherein the gateway maintains a global packet log for all traffic.

14. The arrangement of claim 13 wherein the global packet log includes a sample of all traffic seen on the link to which the gateway is connected.

15. The arrangement of claim 14 wherein packet analysis for a particular monitor happens by classifying packets based on addresses at the time of the analysis.

16. The arrangement of claim 13 wherein the gateway maintains duplicate packets, keeping both a global packet log and a packet log for each virtual monitor.

17. The arrangement of claim 12 wherein the gateway is a clustered gateway and includes a plurality of probes and a cluster head, with the cluster head having a process to aggregate traffic from the probes and to produce separate counter logs for each provisioned customer; and a global counter log, and produce detection heuristics.

Claims 18-23 were objected to as being dependent on a rejected base claim, but containing allowable subject matter.

24. A method of thwarting attacks on a victim data center coupled to a network comprises:

collecting statistical information for a plurality of provisioned customers on links that are downstream from links on which collecting occurs; and

maintaining separate counter logs for each provisioned customer; and a global counter log that accounts for all traffic seen on the links on which collecting occurs.

25. The method of claim 24 wherein collecting occurs on a gateway that passes network packets, the gateway being disposed at an edge of the network.

There was no claim 26 as filed and the examiner elected to re-number the claims at allowance.

27. The method of claim 24 wherein collecting occurs on a data collector that samples network packets, the data collector being disposed at a location that is at a large aggregation link in the network for the data center.

28. The method of claim 24 further comprising:

performing, by the provisioned gateway, intelligent traffic analysis and filtering to identify the malicious traffic and to eliminate the malicious traffic.

29. A method of thwarting attacks on a victim data center coupled to a network comprises:

collecting statistical information for a plurality of links that are downstream from links on which collecting occurs;

performing traffic analysis on the collected statistical information on a per downstream link basis to identify malicious traffic; and

communicating alerts that arise from the traffic analysis.

30. The method of claim 28 wherein performing analysis occurs on statistical information collected for an individual one of the downstream links to identify malicious traffic intended for the individual one of the downstream links.

31. The method of claim 28 wherein communicating to a control center occurs on a downstream link basis.

32. The method of claim 28 wherein communicating occurs on a downstream link basis to a control center that determines a response to the attack.

33. The method of claim 28 wherein communicating occurs on a downstream link basis over a dedicated, hardened network to a control center that determines a response to the attack.

34. The method of claim 28 further comprising:

filtering the identified malicious traffic and to eliminate the malicious traffic from reaching the one of the downstream links.

Evidence Appendix

None

Related Proceedings Appendix

None